REMARKS:

This paper is herewith filed in response to the Examiner's final Office Action mailed on October 28, 2008 for the above-captioned U.S. Patent Application. This office action is a final rejection of claims 1-11 of the application.

More specifically, the Examiner has rejected claims 1, 4-5, 7, and 9-11 under 35 USC 102(a) as anticipated by Relander (US20020066012); and rejected claims 2-3, 6, and 8 under 35 USC 103(a) as being unpatentable over Relander in view of Papineau (US7,092,703). The Applicant respectfully disagrees with the rejection.

Claims 1, 4-5, 7-9, and 11 have been amended for clarification. Claims 1-4 and 6-9 have been amended to address formalities. Support for the amendments can be found at least in paragraphs [0051]-[0052], [0061]-[0063], and [0066]. No new matter is added.

As amended, claim 1 recites:

> "A system configured to arrange end-to-end encryption between two or more pieces of terminal equipment communicating with one another, said terminal equipment comprising: a codec configured to convert an audio signal into a dataflow and vice versa, a module configured to manage encryption parameters stored in connection with the terminal equipment, an encryption key stream generator configured to generate a key stream segment with the said encryption parameters, a module configured to encrypt a dataflow and decrypt the encryption with the generated key stream segment, a module configured to synchronize the encrypted dataflow and to de-synchronize the synchronization, and at least one interface configured to receive the encryption parameters from the data communication network, and wherein at least one of the pieces of terminal equipment is configured to function as a special server terminal device being configured to manage at least one of encryption and synchronization applications as well as the encryption parameters concerning a data communication network and to distribute these based on an established criterion to the other pieces of terminal equipment, and wherein the terminal equipment is configured to download said applications from said special terminal device and to manage said applications, where the terminal equipment comprises a data memory configured to store the applications and a processor and operating memory configured to

execute the applications."

The Applicant notes that the Examiner appears to hold his opinion regarding Relander (US 2002/0066012). In the rejection, the Examiner appears to equate the key stream generator and the synchronization control of Relander to **applications** located in a mobile station or terminal device. The Applicant submits that the rejection of claim 1 appears to improperly apply that the key stream generator and the synchronization control, of Relander, are equivalent to, and perform the functionality of, encryption and synchronization applications, as in claim 1.

Further, the Applicant notes that the Examiner appears to equate the key stream generator and the synchronization control of Relander to "applications" that receive (or download) the initialization vector to start synchronization and also manage the data.

The Applicant disagrees with the rejection. The Applicant submits that Relander can not be seen to disclose or suggest at least where claim 1 relates to terminal equipment configured to download applications from a special terminal device and to manage said applications.

The Applicant submits that, as at least cited below, the pending application clearly discloses what is meant by an "application" according to the exemplary embodiments of the invention.

> "the encryption is carried out at software level at the terminal equipment. Compared with state-of-the-art encryption at hardware level, this achieves dynamic encryption applications for the terminal equipment, whereby it is especially effortless to update the applications," (par. [0033]);
>
> "special server terminal device 15 can be, for example, a data terminal device, which is connected to the data communication network 10 and in connection with which storing means [...] especially storing dynamic encryption applications 32," and "such applications are arranged, which can be transferred to pieces of terminal equipment,..., such as e.g. algorithms used for generation of an encryption key flow or for encryption of the actual dataflow,"(pars. [0050] and [0052]);
>
> "the terminal equipment 11.1, 11.2 includes a connection interface for external data terminal equipment (DTE) 26, which can be used for downloading

> encryption information, such as keys and applications, in the terminal equipment 11.1, 11.2 from the server terminal device 15 or such," (par. [0066]);
>
> "Downloading of applications 32 in pieces of terminal equipment 11.1, 11.2 can also be performed locally," (par. [0057]); and
>
> "Updating of the encryption keys 19 and the applications 32 used in the encryption (key stream generator, KSG) is thus performed for the SIM module 28 of terminal equipment 11.1, 11.2," (par. [0061]).

The Applicant submits that, as supported in the pending application, it is easily realized that an "application" is easily downloadable and updateable. In accordance with the exemplary embodiments of the invention, at least one of the terminals stores encryption and synchronization applications to be transmitted to the other terminals, and the other terminals are downloading such transmitted encryption and synchronization applications.

The Applicant submits that the encryption key stream generator and the synchronization control of Relander can not be seen to relate **encryption and synchronization applications** as in claim 1. Rather, the key stream generator and the synchronization control of Relander are seen to relate to hardware components which can not be downloaded from another device. The Applicant notes that what is actually downloaded (or transmitted) in Relander is merely a synchronization vector [0032]. This synchronization vector appears to be the only data to be used by key stream generator.

The Applicant contends that, for at least the reasons already stated, Relander can not be seen to disclose or suggest a special terminal server "being configured to manage at least one of **encryption and synchronization applications** as well as the encryption parameters concerning a data communication network **and to distribute these based on an established criterion to the other pieces of terminal equipment**," as in claim 1.

The Applicant submits that this distinction has been made more apparent in the amended claim 1.

For at least the reasons stated the rejection of claim 1 is seen as improper and the rejection should

be removed.

Regarding the rejection of claim 5, the Applicant submits that for at least the reasons stated above Relander can not be seen to disclose or suggest at least where the apparatus of claim 5 relates to "a module configured to **download and manage encryption and synchronization applications as well as encryption parameters**, wherein a functionality of the apparatus to carry out end-to-end encrypted communication with another apparatus is implemented by the at least one of encryption and synchronization applications based on the at least one encryption parameter." Thus, the rejection of claim 5 should be removed.

Further, for at least the reasons already stated the Applicant submits that the references cited are not seen to disclose or suggest at least where claim 7 recites "**receiving from a data communication network information comprising at least one of encryption and synchronization applications as well as encryption parameters,** and at least one encryption key." For at least this reason the rejection of claim 7 should be removed.

In addition, for at least the reasons stated the references cited are not seen to disclose or suggest at least where claim 11 recites "managing at least one of **encryption and synchronization applications as well as encryption parameters** concerning a data communication network; and **distributing the at least one of encryption and synchronization applications as well as the encryption parameters based on an established criterion to pieces of terminal equipment**." For at least this reason the rejection of claim 11 should be removed.

Papineau relates to a method to input and output data to/from Java MIDlets (abstract). Further, Papineau discloses that as a current security measure MIDlets downloaded and installed on a local file system can only access limited resources (col. 13, lines 4-18). Although the Applicant does not agree that a combination of Relander and Papineau is proper, the Applicant submits that such a combination would still address the deficiencies of Relander as stated above.

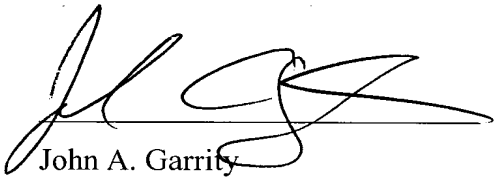
In addition, for at least the reason that claims 2-4, 6, and 8-10 depend from claims 1, 5, and 7 the

references cited are not seen to disclose or suggest these claims.

Based on the above explanations and arguments, it is clear that the references cited cannot be seen to disclose or suggest claims 1-11. The Examiner is respectfully requested to reconsider and remove the rejections of claims 1-11 and to allow all of the pending claims 1-11 as now presented for examination.

For all of the foregoing reasons, it is respectfully submitted that all of the claims now present in the application are clearly novel and patentable over the prior art of record. Should any unresolved issue remain, the Examiner is invited to call Applicants' attorney at the telephone number indicated below.

Respectfully submitted:



11/15/2009

John A. Garrity
Reg. No.: 60,470
Customer No.: 29683
HARRINGTON & SMITH, PC
4 Research Drive
Shelton, CT 06484-6212
Telephone: (203)925-9400
Facsimile: (203)944-0245
email: jgarrity@hspatent.com

Date

S.N.: 10/511,934
Art Unit: 2432

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. BOX 1450, Alexandria, VA 22313-1450.

1/15/2009 — Date

Claire F. Main — Name of Person Making Deposit